Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of
Baltimore City Police Department
Baltimore, Maryland

Complaint for Relief Against
Unauthorized Radio Operation and
Willful Interference with Cellular
Communications

Petition for an Enforcement Advisory
on Use of Cell Site Simulators by State
and Local Government Agencies

Memorandum in Support of Complaint for Relief Against Unauthorized Radio Operation and Willful Interference with Cellular Communications and Petition for an Enforcement Advisory on Use of Cell Site Simulators by State and Local Government Agencies

(Complaint and Petition Submitted August 16, 2016)

Submitted by
American Civil Liberties Union
American Civil Liberties Union of Northern California
New York Civil Liberties Union
American Civil Liberties Union of Maryland
Electronic Frontier Foundation

Nathan Freed Wessler
American Civil Liberties Union Foundation
125 Broad St., 18th Fl.
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

September 1, 2016

Additional Signatories Listed Below

Table of Contents

Summary 1

Interest of Parties 3

Argument 4

I. The Issues Identified in the Complaint and Petition Are National in Scope and Require Definitive Action by the FCC. 4

A. Police departments all across the country use cell site simulators with great frequency, for non-emergency reasons, and under a veil of extraordinary secrecy that is ripe for discriminatory abuse. 4

B. The FCC has enabled widespread use and concealment of cell site simulators, and should act immediately to conform state and local law enforcement's activities to the law. 19

II. The Use of Cell Site Simulators by State and Local Law Enforcement Agencies Violates Sections 301 and 333 of the Communications Act 24

III. Any System for Granting Cell Site Simulator Use Licenses to State and Local Law Enforcement Agencies Must Be Predicated on Strong Transparency, Accountability, and Oversight to Protect Against Abuse. 32

Conclusion 36

The American Civil Liberties Union, American Civil Liberties Union of Northern California, New York Civil Liberties Union, and American Civil Liberties Union of Maryland (collectively, "ACLU") and the Electronic Frontier Foundation ("EFF") respectfully urge the Federal Communications Commission ("FCC" or "Commission") to take immediate action to end ongoing violations of the Communications Act by state and local law enforcement agencies that possess and use cell site simulator devices. The ACLU and EFF submit this filing in support of the Complaint for Relief Against Unauthorized Radio Operations and Willful Interference with Cellular Communications by the Baltimore Police Department and Petition for an Enforcement Advisory on Use of Cell Site Simulators by State and Local Government Agencies ("Complaint" or "Complaint and Petition") submitted by the Center for Media Justice, Color Of Change, and the Open Technology Institute at New America on August 16, 2016.[1]

Summary

As explained in the Complaint and Petition, cell site simulators are devices that mimic cellular base stations and force cell phones in the area to broadcast their unique identifying information (such as their International Mobile Subscriber Identity) to the government's device. As part of their operation, cell site simulators can interfere with cellular communications, and can disrupt the ability of nearby phones to make and receive calls. Moreover, the Complaint demonstrated serious concerns about racially disparate impact of cell site simulator use by law enforcement in Baltimore.

---

[1] *In re Baltimore City Police Department, Baltimore, Maryland*, Complaint for Relief Against Unauthorized Radio Operations and Willful Interference with Cellular Communications and Petition for an Enforcement Advisory on Use of Cell Site Simulators by State and Local Government Agencies (FCC Aug. 16, 2016), https://www.fcc.gov/ecfs/filing/10816659216934/document/10816659216934dd54.

The ACLU and EFF submit this filing in support of the Complaint and Petition to illustrate that the Baltimore Police Department is far from the only law enforcement agency to make heavy use of the technology. Dozens of police departments across the country, from Boston to San Diego and from Anchorage to Miami, have used cell site simulators for years, but have shrouded their acquisition and use of the technology in great secrecy, thereby avoiding effective oversight by local lawmakers, judges, and the public. Only with transparency and oversight can the privacy and integrity of Americans' cellular communications be protected.

Because state and local law enforcement agencies do not hold FCC licenses to operate cell site simulators over the wireless spectrum, and because the technology interferes with cellular communications, use of the devices by state and local authorities violates Sections 301 and 333 of the Communications Act. The technology is widely and frequently used by state and local law enforcement agencies across the country in violation of the law, however.

The ACLU and EFF present recommendations for FCC action on this issue, including the immediate cessation of operation of cell site simulators by state and local law enforcement agencies, at least until a proper licensing procedure that provides for necessary oversight and safeguards is put in place. The FCC should issue an enforcement advisory to end these ongoing violations immediately. Moreover, any licensing scheme put in place by the FCC to allow state and local agencies to operate cell site simulators must be predicated on strong protections to minimize interference with cellular communications, to facilitate proper oversight from local elected lawmakers and from courts, and to ensure transparency to the public.

Interest of Parties

For nearly 100 years, the American Civil Liberties Union has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country. The ACLU takes up the toughest civil liberties cases and issues to defend all people from government abuse and overreach. With more than a million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for the principle that every individual's rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin. The American Civil Liberties Union of Northern California, New York Civil Liberties Union, and American Civil Liberties Union of Maryland are affiliates of the ACLU.

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for more than 25 years. With roughly 27,000 active donors and dues-paying members nationwide, EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law in the digital age. EFF regularly serves as counsel or *amicus* in state and federal cases involving the application of the Fourth Amendment to new technologies such as cell phone location information, and has for years contributed its expertise in law, regulation, and technology to representing consumers before this and other agencies on the issues of innovation, competition, and privacy.

Argument

I. The Issues Identified in the Complaint and Petition Are National in Scope and Require Definitive Action by the FCC.

A. Police departments all across the country use cell site simulators with great frequency, for non-emergency reasons, and under a veil of extraordinary secrecy that is ripe for discriminatory abuse.

As explained in the Complaint, the Baltimore Police Department appears to have used cell site simulators with greater frequency and volume than any other state or local law enforcement agency for which public data is currently available and in a manner that disproportionately affects people of color. The ACLU and EFF submit these comments to explain underlying concerns with the use of cell site simulators, which led to the results detailed in the Complaint and Petition. Three aspects of law enforcement's use of the technology are particularly troubling: State and local agencies use the device with great frequency, for a wide array of non-emergency purposes, and under a veil of extraordinary secrecy that is ripe for discriminatory abuse. Baltimore Police are far from the only law enforcement agency to make heavy use of the technology, however. At last count, the ACLU was aware of 66 state and local law enforcement agencies in 23 states and the District of Columbia that own cell site simulators.[2] This includes both large and small agencies, from major police departments in cities like New York and Oakland, to smaller agencies in Sunrise, Florida, Tempe, Arizona, and elsewhere. The available data almost certainly represents a dramatic undercount, as many agencies continue to conceal their purchase and use of the technology from the public.

Records from police departments across the country that have disclosed information about their use of cell site simulators show that the equipment is typically used with frequency.

[2] *Stingray Tracking Devices: Who's Got Them?*, ACLU, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them.

In New York City, for example, the police department used cell site simulators more than 1,000 times over seven years.[3] In Tacoma, Washington, it was used more than 170 times in five years,[4] and in Tallahassee, Florida, the police department used cell site simulators to track 277 phones over a six-and-a- half-year period.[5] The Michigan State Police used cell site simulators 128 times in a recent one-year period,[6] and in Kansas City, Missouri, police had used them 97 times as of 2015.[7] The Milwaukee Police Department used cell site simulators in 579 investigations over five years,[8] and the Charlotte-Mecklenburg Police Department in North Carolina requested court authorization to do so more than 500 times over a similar period.[9] In California, the Sacramento Sheriff's Department initially estimated that it used cell site simulators in about 500 criminal

---

[3] Joseph Goldstein, *New York Police Are Using Covert Cellphone Trackers, Civil Liberties Group Says*, N.Y. Times, Feb. 11, 2016, http://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html.

[4] Adam Lynn, *Tacoma Police Change How They Seek Permission to Use Cellphone Tracker*, News Tribune, Nov. 15, 2014, http://www.thenewstribune.com/news/local/crime/article25894096.html.

[5] Log of Tallahassee Police Department Use of Cell Site Simulators, Released Pursuant to ACLU Public Records Request, https://www.aclu.org/files/assets/floridastingray/03.27.2014%20-%20Master%20CE%20Log.pdf.

[6] Joel Kurth, *Michigan State Police Using Cell Snooping Devices*, Detroit News, Oct. 23, 2015, http://www.detroitnews.com/story/news/local/michigan/2015/10/22/stingray/74438668/.

[7] Glenn E. Rice, *Secret Cellphone Tracking Device Used by Police Stings Civil Libertarians*, Kan. City Star, Sept. 5, 2015, http://www.kansascity.com/news/business/technology/article34185690.html.

[8] Nathan Freed Wessler, *New Evidence Shows Milwaukee Police Hide Stingray Usage From Courts and Defense*, Free Future Blog, ACLU, Jan. 25, 2016, https://www.aclu.org/blog/free-future/new-evidence-shows-milwaukee-police-hide-stingray-usage-courts-and-defense.

[9] Fred Clasen-Kelly, *CMPD's Cellphone Tracking Cracked High-Profile Cases*, Charlotte Observer, Nov. 22, 2014, http://www.charlotteobserver.com/news/local/crime/article9235652.html.

cases, but later said it could be up to 10,000.[10] The Baltimore County Police Department used cell site simulators 622 times over five years,[11] while elsewhere in Maryland the Howard County Police deployed cell site simulators 129 times over four years.[12] The Oakland Police Department has never disclosed the number of times the device has been used, but has admitted using it in connection with 59 arrests over a three-year period.[13] It was recently revealed that for one such arrest in 2013, the cell site simulator may have been in use continuously for up to 10 hours without a warrant.[14]

Equipment manufacturer Harris Corporation represented to the FCC in applying for equipment authorizations that the "only" "purpose" was "to provide state/local law enforcement officials with authority to utilize this equipment in *emergency* situations." (Emphasis added.)[15] But far from reserving this technology for only life-and-death emergencies, counterterrorism operations, or other critical uses, police departments have used cell site simulators in the full

---

[10] *New Developments in Sacramento "Stingray" Case*, ABC 10, Jan. 8, 2016, http://www.abc10.com/news/local/sacramento/new-developments-in-sacramento-stingray-case/24444110.

[11] Alison Knezevich, *Baltimore Co. Police Used Secretive Phone-Tracking Technology 622 Times*, Baltimore Sun, Apr. 9, 2015, http://www.baltimoresun.com/news/maryland/crime/bs-md-co-county-stingray-20150409-story.html.

[12] Howard County, Filtered Log, https://www.documentcloud.org/documents/2799747-Howard-County-filtered-log.html.

[13] Linda Lye, *Documents Reveal Unregulated Use of Stingrays in California*, ACLU of Northern California Blog, Mar. 14, 2014, https://www.aclunc.org/blog/breaking-documents-reveal-unregulated-use-stingrays-california.

[14] Cyrus Farivar, *FBI's Stingray Quickly Found Suspect After Local Cops' Device Couldn't*, Ars Technica, Aug. 26, 2016, http://arstechnica.com/tech-policy/2016/08/to-find-suspect-city-cops-ran-stingray-for-hours-then-called-in-fbi/.

[15] Nicole Ozer, *Documents Suggest Maker of Controversial Surveillance Tool Misled the FCC*, ACLU of Northern California Blog, Sept. 17, 2014, https://www.aclunc.org/blog/documents-suggest-maker-controversial-surveillance-tool-misled-fcc (discussing documents obtained from FCC through Freedom of Information Act request).

range of run-of-the-mill criminal investigations. For example, "[o]ut of 128 investigations where [the Michigan State Police] used Stingrays in 2014, 42 were related to homicides, 30 for burglaries and robberies, 12 for assaults, 11 for missing persons, and the rest for a mix of offenses including drug crimes, obstructing police, and fraud."[16] In New York City, the NYPD used its cell site simulators to track suspects in crimes ranging from identity theft, drug offenses, robbery, and criminal contempt of court, to assault and homicide.[17] In Tacoma, Washington, the overwhelming majority of cell site simulator deployments in the first half of 2014 were for drug investigations—far more than for homicides or other categories of crimes.[18] Likewise the Howard County, Maryland, Police Department "investigated more drug cases with its devices than any other type of crime. Of the 41 drug cases, which represent a little more than 30 percent of the investigations, police made only one arrest."[19] In Tallahassee, cell site simulators were used to investigate financial crimes, "wanted person[s]," and property crimes, in addition to crimes of violence.[20] In Baltimore, "[t]he most common use by far was solving robberies."[21] In

---

[16] Nathan Freed Wessler, *Police Citing "Terrorism" to Buy Stingrays Used Only for Ordinary Crimes*, ACLU Free Future Blog, Oct. 23, 2015, https://www.aclu.org/blog/free-future/police-citing-terrorism-buy-stingrays-used-only-ordinary-crimes.

[17] *Over the Air Intercepts* (2008–2015), New York Police Department, http://www.nyclu.org/files/summary_overtheairintercept_web.pdf (obtained via public records request by the New York Civil Liberties Union).

[18] *Police are Using a Powerful Surveillance Tool to Fight the War on Drugs, Not Terrorism*, Privacy SOS, Oct 15, 2014, https://privacysos.org/blog/police-are-using-a-powerful-surveillance-tool-to-fight-the-war-on-drugs-not-terrorism/.

[19] Courtney Mabeus, *Battlefield Technology Gets Spotlight in Maryland Courts: Secrecy and Defense Concerns Surround Cell Phone Trackers*, Capital News Service, May 3, 2016, https://web.archive.org/web/20160504160050/http://cnsmaryland.org/interactives/spring-2016/maryland-police-cell-phone-trackers/index.html.

[20] Log of Tallahassee Police Department Use of Cell Site Simulators, *supra*.

Annapolis, Maryland, police deployed their cell site simulator "in the case of a Pizza Boli's employee who reported being robbed of 15 chicken wings and three subs while out on delivery."[22] Tacoma police used a cell site simulator to search for a stolen city laptop.[23]

These concerns about use of cell site simulators are heightened by the fact that many of the police departments known to possess the technology have a documented history of discriminatory and racially biased policing.[24] The Commission has an obligation to ensure that

---

[21] Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA Today, Aug. 24, 2015, http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/.

[22] Mabeus, *Battlefield Technology Gets Spotlight in Maryland Courts*, *supra*.

[23] Tacoma, Washington, Log of Cell Site Simulator Uses, 2009–2014, https://muckrock.s3.amazonaws.com/foia_files/partial_response.pdf (entry for 6/10/2010).

[24] *See, e.g.*, Complaint at 20–24 (discussing racially disparate impact of cell site simulator use in Baltimore); *Report of the Blue Ribbon Panel on Transparency, Accountability, and Fairness in Law Enforcement*, City and County of San Francisco (2016), http://sfblueribbonpanel.com/ (finding racial disparities in San Francisco Police Department stops, searches, and arrests); *Executive Summary: The Stanford Reports on Improving Police-Community Relations in Oakland, California*, Stanford SPARQ (2016), https://stanford.app.box.com/v/OPD-Executive-Summary ("[Oakland Police Department] officers stopped, searched, handcuffed, and arrested more African Americans than Whites, a finding that remained significant even after we controlled for neighborhood crime rates and demographics; officer race, gender, and experience; and other factors that shape police actions."); Jeffrey Fagan et al., *Final Report: An Analysis of Race and Ethnicity Patterns in Boston Police Department Field Interrogation, Observation, Frisk, and/or Search Reports* (2015), https://s3.amazonaws.com/s3.documentcloud.org/documents/2158964/full-boston-police-analysis-on-race-and-ethnicity.pdf (finding "racially disparate treatment" of Black and Latino people by Boston Police Department); *Floyd v. City of New York*, 959 F. Supp. 2d 540 (S.D.N.Y. 2013) (finding racial bias in NYPD "stop and frisk" activities); New York Civil Liberties Union, *Beyond "Deliberate Indifference": An NYPD for All New Yorkers* (2013), http://www.nyclu.org/files/publications/nypd_report_final_0.pdf (detailing disproportionate targeting of Black, Latino, and Muslim communities by NYPD); *Ortega Melendres v. Arpaio*, 989 F. Supp. 2d 822 (D. Ariz. 2013) (finding that the Maricopa County Sheriff's Office had relied on racial profiling and illegal detentions to target Latinos); Ben Poston, *Racial Gap Found in Traffic Stops in Milwaukee*, Journal Sentinel, Dec. 3, 2011, http://archive.jsonline.com/watchdog/watchdogreports/racial-gap-found-in-traffic-stops-in-milwaukee-ke1hsip-134977408.html ("A black Milwaukee driver is seven times as likely to be stopped by city police as a white resident driver, a Journal Sentinel analysis of nearly 46,000

the impacts of use of this invasive and widely deployed technology do not fall disproportionately on communities of color.[25]

Despite the widespread and workaday uses of cell site simulators, law enforcement agencies have consistently hidden basic information about their use of the technology from lawmakers, judges, and the public. In Maryland, for example, during a 2014 legislative hearing a representative of the State Police refused to answer a state senator's question about law enforcement use of cell site simulators on the grounds that such information was "classified."[26] In Tacoma, Washington, after the local newspaper revealed that the police department had been using a cell site simulator, city council members told a reporter that they "didn't know what they were buying" when they approved the cell site simulator purchase, apparently because the police department failed to provide an adequate explanation.[27]

In Santa Clara County, California, local lawmakers tried to learn basic information about how the cell site simulator would work and asked to have a demonstration before voting on whether to approve its purchase. This request was denied and the lawmakers were told that a

---

traffic stops has found. Similarly, Milwaukee police pulled over Hispanic city motorists nearly five times as often as white drivers, according to the review.").

[25] *See* Complaint at 34–36.

[26] *Electronic Device Location Information: Hearing on SB 698 Before the Sen. Judicial Proceedings Comm.*, 2014 Reg. Session (Md. Mar. 6, 2014) (3:03:15–3:04:07 of recording), http://mgaleg.maryland.gov/webmga/frmMain.aspx?pid=billpage&stab=01&id=sb0698&tab=subject3&ys=2014RS (Senator Shank: "Does the Maryland State Police employ this [Stingray] technology at this time?" Sgt. Bonner: "Do we employ the actual technology of a Stingray device? I can't comment on that at this time." Sen. Shank: "Is it classified?" Sgt. Bonner: "It is classified.").

[27] Kate Martin, *Documents: Tacoma Police Using Surveillance Device to Sweep Up Cellphone Data*, News Tribune, Aug. 26, 2014, http://www.thenewstribune.com/news/local/article25878184.html.

demonstration was open to "only people with badges."[28] At a 2015 legislative hearing, Supervisor Joe Simitian summarized the situation: "[s]o, just to be clear, we are being asked to spend $500,000 of taxpayers' money and $42,000 a year thereafter for a product for the name brand which we are not sure of, a product we have not seen, a demonstration we don't have, and we have a nondisclosure requirement as a precondition. You want us to vote and spend money, [but] you can't tell us more about it."[29]

Some local lawmakers may not even be aware that cell site simulators are available to law enforcement entities in their community. For example, the Anaheim, California, Police Department made its arsenal of cell site simulators available to law enforcement in neighboring jurisdictions, leaving elected leaders and millions of Orange County residents with no opportunity to weigh in on the technologies' acquisition or use.[30]

Police departments have consistently hidden their use of cell site simulators from judges and defense counsel, as well, meaning that it has been exceedingly rare for courts to have an opportunity to evaluate the legality of cell site simulator surveillance. The overwhelming majority of publicly available examples of applications for court orders by state and local authorities fail to explain that police intended to use a cell site simulator, the capabilities of the device, or its effects on bystanders' phones. Law enforcement agents have generally applied for

---

[28] Matt Richtel, *A Police Gadget Tracks Phones? Shhh! It's Secret*, N.Y. Times, Mar. 15, 2015, http://www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html?_r=0.

[29] *Id.*

[30] Matt Cagle, *Dirtbox Over Disneyland? New Docs Reveal Anaheim's Cellular Surveillance Arsenal*, ACLU of Northern California Blog, Jan. 27, 2016, https://www.aclunc.org/blog/dirtbox-over-disneyland-new-docs-reveal-anaheim-s-cellular-surveillance-arsenal.

pen register orders rather than warrants,[31] and those pen register applications have appeared on their face to seek authority to obtain information, including cell phone location information, from the suspect's cellular service provider. They have not put judges on notice that police intended to use their own device that bypasses the phone company by impersonating its equipment, queries multiple nearby phones, and interferes with cellular service in the area. Thus, for example, in Tacoma, judges "unwittingly signed more than 170 orders" without knowing "that they'd been authorizing Tacoma police to use a device capable of tracking someone's cellphone" because "police never mentioned they intended to use the device when detectives swore out affidavits seeking so-called 'pen register, trap and trace' orders allowing them to gather information about a suspect's cellphone use and location."[32] After a local newspaper investigation revealed that police had relied on these orders to justify cell site simulator use, local judges collectively imposed a requirement that the government spell out whether it is seeking to use a cell site simulator in future applications and imposed limits on retention of bystanders' data.[33] Those rules and others were later enshrined in state law.[34]

In Charlotte, "[t]he court orders that authorize the surveillance do not mention StingRays or explain that the device captures cellphone data from both criminal suspects and innocent people."[35] It was only after reading about law enforcement's use of cell site simulators in the local newspaper that a judge "rejected an application from CMPD to conduct the cellphone

---

[31] Pen register orders are issued upon a showing "that the information likely to be obtained is relevant to an ongoing criminal investigation," 18 U.S.C. § 3122(b)(2), rather than the probable cause required for a warrant.

[32] Lynn, *Tacoma Police Change*, *supra.*

[33] *Id.*

[34] Wash. Rev. Code § 9.73.260.

[35] Clasen-Kelly, *CMPD's Cellphone Tracking*, *supra.*

surveillance. It was a first for police."[36] In Sacramento, law enforcement "never told judges or prosecutors that they were using the so-called 'cell site simulators' - nor did they specifically ask for permission to use one."[37] In the Northern District of California, federal prosecutors acknowledged that they had been submitting pen register applications to federal magistrate judges to justify cell site simulator use, "although the pen register application[s] do[] not make that explicit."[38] In a case in Arizona, a federal prosecutor belatedly admitted that "there was not a full disclosure to the magistrate judge with respect to the nature and operation of the [cell site simulator] device."[39]

A Baltimore case illustrates the typical lack of government candor.[40] The pen register application submitted by police in the case primarily sought authority to obtain information from a cellular service provider. In a single paragraph, the government additionally sought permission to "initiate a signal to determine the location of the subject's mobile device on the service provider's network or with such other reference points as may be reasonably available, Global Position System Tracing and Tracking, Mobile Locator tools, R.T.T. (Real Time Tracking Tool),

---

[36] *Id.*

[37] *New Developments in Sacramento "Stingray"Case*, *supra.*

[38] Linda Lye, *Justice Department Emails Show Feds Were Less Than "Explicit" with Judges on Cell Phone Tracking Tool*, ACLU of Northern California Blog, Mar. 27, 2013, https://aclunc.org/blog/justice-department-emails-show-feds-were-less-explicit-judges-cell-phone-tracking-tool.

[39] Motion Hr'g Tr. at 81, *United States v. Rigmaiden*, No. CR 08-00814 (D. Ariz. Mar. 28, 2013), https://ia600707.us.archive.org/33/items/gov.uscourts.azd.396130/gov.uscourts.azd.396130.1004.0.pdf.

[40] *See State v. Andrews*, 134 A.3d 324 (Md. Ct. Spec. App. 2016).

. . . Precision Locations and any and all locations . . . ."[41] The application contained no explanation of what these "tools" were, how they operated, how they would be used, or that they would interfere with cellular communications in the area. On appeal, the Maryland Court of Special Appeals excoriated the government for "fail[ing] to provide the necessary information upon which the court could make the constitutional assessments mandated in this case."[42] The court's role in assessing the government's action "requires analysis of the functionality of the surveillance device and the range of information potentially revealed by its use," and the government's failure to "provid[e] details sufficient to assure the court that a novel method of conducting a search is a reasonable intrusion made in a proper manner and justified by the circumstances, obstructs the court's ability to make the necessary constitutional appraisal."[43]

In Baltimore, as elsewhere, law enforcement has consistently hidden its use of cell site simulators at all stages of investigations and court proceedings, from pen register applications and resulting investigative reports, to subsequent arrest warrant affidavits and court hearings. An investigation by USA Today found that across hundreds of cases in Baltimore, police "concealed" their use of cell site simulators "from the suspects, their lawyers and even judges":

> In court records, police routinely described the phone surveillance in vague terms— if they mentioned it at all. In some cases, officers said only that they used "advanced directional finding equipment" or "sophisticated electronic equipment" to find a suspect. In others, the police merely said they had "located" a suspect's

---

[41] Application, *In re Application of the State of Maryland for an Order Authorizing the Installation and Use of a Device Known as a Pen Register/Trap & Trace Over 443-208-2776*, at 4–5 (Cir. Ct. for Balt. City, Md., May 5, 2014), https://www.aclu.org/legal-document/baltimore-police-department-application-pen-register-order.

[42] *Andrews*, 134 A.3d at 339.

[43] *Id.* at 338–39 (internal quotation marks omitted).

> phone without describing how, or they suggested they happened to be in the right place at the right time.[44]

Baltimore police officers have also refused to answer questions under oath in pretrial hearings, citing "Homeland Security issues" and a non-disclosure agreement with the FBI, and prosecutors even have withdrawn cell site simulator-derived evidence rather than see judges sanction those refusals to answer with contempt findings or exclusion of evidence.[45] As has been the case elsewhere in the country, Baltimore police and prosecutors consistently failed to provide notice to people tracked and located using cell site simulators, or to disclose information about use of the cell site simulator to the defense in pre-trial discovery.[46]

Similarly, in Sarasota, Florida, internal police emails show that, at the request of the U.S. Marshals Service, local law enforcement omitted mention of cell site simulators from probable cause affidavits, reports, and depositions. Instead, their practice was to say they had

---

[44] Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA Today, Aug. 24, 2015, http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/.

[45] Justin Fenton, *Judge Threatens Detective with Contempt for Declining to Reveal Cellphone Tracking Methods*, Balt. Sun, Nov. 17, 2014, http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-officer-contempt-20141117-story.html.

[46] *See* Jessica Anderson, *Public Defender's Office to Review Cases Involving Stingray Technology,* Aug. 28, 2015, http://www.baltimoresun.com/news/maryland/crime/bs-md-stingray-cases-20150828-story.html (explaining that "[t]he Baltimore public defender's office said it plans to review nearly 2,000 cases in which police used a controversial cellphone surveillance tool without defense attorneys' knowledge" and quoting defense attorney describing lack of disclosures as "a national problem"). Even the U.S. Department of Justice policy guidance on cell site simulators fails to require notice to people who are located using the technology. *See* Dep't of Justice, *Policy Guidance: Use of Cell-Site Simulator Technology*, at 2, 5 (Sept. 3, 2015), https://www.justice.gov/opa/file/767321/download.

"received information from a confidential source regarding the location of the suspect."[47] In a Tallahassee case where cell site simulator use was later revealed, a police officer under deposition would say only that "covert investigative techniques were used to locate the cell phone," and refused to "go into detail" to describe them.[48] Investigative reports from other Tallahassee cases where police used cell site simulators omit mention of the technology, instead alluding only to use of "electronic surveillance measures," "confidential intelligence," or nothing at all.[49]

Even when the government has informed judges that it intended to use a cell site simulator, it has often provided insufficient information about how the technology operates and its effects on third parties for the court to make an informed decision about whether and how to authorize its use.[50] Indeed, the language used by federal law enforcement agencies when applying for cell site simulator warrants appears to understate the degree to which the

---

[47] Maria Kayanan, *Internal Police Emails Show Efforts to Hide Use of Cell Phone Tracking*, Free Future Blog, ACLU, June 19, 2014, https://www.aclu.org/blog/internal-police-emails-show-efforts-hide-use-cell-phone-tracking.

[48] *See* Def.'s Mot. to Compel Disclosure of Evidence, *State v. Thomas*, No. 2008-CF-3350 (Fla. 2d Cir. Ct. Aug. 2, 2010), https://www.aclu.org/legal-document/defendants-motion-compel-disclosure-evidence-state-v-thomas.

[49] Nathan Freed Wessler, *ACLU-Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida*, Free Future Blog, ACLU, Feb. 22, 2015, https://www.aclu.org/blog/free-future/aclu-obtained-documents-reveal-breadth-secretive-stingray-use-florida.

[50] *See, e.g.*, *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d 747, 749 (S.D. Tex. 2012) ("The application has a number of shortcomings. It does not explain the technology, or the process by which the technology will be used to engage in the electronic surveillance to gather the Subject's cell phone number.").

technology interferes with cellular communications, and omits any discussion of the risk of interference with 911 calls or other emergency communications.[51]

The extreme secrecy surrounding use of cell site simulators has stymied effective oversight and left Americans' cellular communications without sufficient protections against interference. We are aware only of a handful of jurisdictions where lawmakers and the public have been presented with *any* information about cell site simulators prior to purchase or use. The importance of transparency and public debate is demonstrated by the experience in these few jurisdictions. Where legislative hearings and public debate have occurred, essential questions have been asked about how the technology will be used and how people's rights will be protected. These communities have determined that the equipment should not be purchased at all or have enacted comprehensive safeguards designed to prevent discriminatory use and provide transparency, oversight, and accountability.

In Santa Clara, County, California, for example, members of the Board of Supervisors learned that the Sheriff intended to purchase a cell site simulator and asked questions about the secrecy of the project, the expense, and the privacy and civil rights implications of the system. Members of the Board questioned how they could be asked to approve a technology that was

---

[51] *Compare* Affidavit in Support of Application for a Search Warrant, ¶ 54, *In re Use of a Cell Site Simulator to Locate the Cellular Device Assigned Call Number (910) 850-4060*, No. 5:15-MJ-2282 (E.D.N.C. Dec. 16, 2015), https://www.aclu.org/legal-document/affidavit-support-application-search-warrant-cell-site-simulator ("Any service disruption to non-target devices will be brief and temporary . . . ."), *with* Colin Freeze, *RCMP Listening Device Capable of Knocking Out 911 Calls, Memo Reveals*, Globe & Mail, Apr. 18, 2016, http://www.theglobeandmail.com/news/national/rcmp-listening-tool-capable-of-knocking-out-911-calls-memo-reveals/article29672075/ (describing internal Royal Canadian Mounted Police memorandum that "says that when the [cell site simulator] device is turned on, it can block new calls on all phones in the vicinity, including attempts to dial 911 . . . .").

shrouded in secrecy even from the Board itself.[52] The County Executive ultimately rejected the purchases because the company selling the cell site simulator refused to "agree to even the most basic criteria we have in terms of being responsive to public records requests. . . . We had to do what we thought was right."[53] The County also noted that its overarching effort to develop policies concerning surveillance technology "will be informed by the discussions that have occurred."[54] In June, 2016, the Santa Clara County Supervisors enacted a landmark law that requires consistent transparency, accountability, and oversight for all surveillance technology proposals, acquisition, and use.[55]

In Oakland, California, recent efforts by local law enforcement to acquire invasive surveillance technology without adequate transparency, accountability, and oversight has led to a City Council-created Privacy Advisory Commission.[56] The Privacy Advisory Commission is currently investigating whether it is appropriate to authorize the Oakland Police Department to

---

[52] Richtel, *A Police Gadget Tracks Phones? Shhh! It's Secret*, *supra*.

[53] Cyrus Farivar, *In Rare Move, Silicon Valley County Gov't Kills Stingray Acquisition*, Ars Technica, May 7, 2015, http://arstechnica.com/tech-policy/2015/05/in-rare-move-silicon-valley-county-govt-kills-stingray-acquisition/.

[54] County of Santa Clara, Update on Acquisition of a Mobile Phone Triangulation System (May 5, 2015), https://www.documentcloud.org/documents/2073952-update-on-acquisition-of-cellphone-triangulation.html.

[55] Nicole A. Ozer, *Santa Clara County Passes Landmark Law to Shut Down Secret Surveillance,* ACLU of Northern California Blog, June 8, 2016, https://www.aclunc.org/blog/santa-clara-county-passes-landmark-law-shut-down-secret-surveillance; *see also Making Smart Decisions About Surveillance: A Guide for Community Transparency, Accountability & Oversight*, ACLU of California, 2d ed., April 2016, https://www.aclunc.org/publications/making-smart-decisions-about-surveillance-guide-community-transparency-accountability.

[56] *Privacy Advisory Commission: What does the Privacy Advisory Commission Do?*, City of Oakland, http://www2.oaklandnet.com/government/o/CityAdministration/d/PrivacyAdvisoryCommission/index.htm.

use a cell site simulator owned by the District Attorney's Office, and if so, what practices and policies would be necessary to safeguard rights.[57] The Privacy Commission is also drafting an ordinance that would ensure consistent public debate, oversight, and accountability for all surveillance technology proposals, acquisitions or uses.[58]

In Hennepin County, Minnesota, news that the Hennepin County Sheriff's Office sought to purchase a cell site simulator led to public debate at county government meetings and passage of an ordinance requiring all future purchases of such equipment be explicitly approved by the county board.[59]

Several state legislatures have also started to take action to address the vacuum of oversight related to the use of cell site simulators by local law enforcement. In Washington State, after local reporters uncovered the surreptitious use of cell site simulators by Tacoma police, the state legislature unanimously enacted a law placing restrictions on use of the technology, including that police must obtain a warrant from a judge and must disclose in their warrant application "any disruptions to access or use of a communications or internet access

---

[57] Darwin BondGraham, *Oakland Privacy Commission Holds Hearing on 'Stingray' Cell Phone Surveillance Devices*, East Bay Express, Aug. 12, 2016, http://www.eastbayexpress.com/SevenDays/archives/2016/08/12/oakland-privacy-commission-holds-hearing-on-stingray-cell-phone-surveillance-devices; Special Meeting Agenda, Privacy Advisory Committee, Aug. 11, 2016, http://www2.oaklandnet.com/oakca1/groups/cityadministrator/documents/agenda/oak060110.pdf .

[58] Matt Cagle, *With DAC Vote, Oakland Shows How Surveillance Reform Begins at Home*, ACLU of Northern California Blog, June 10, 2015, https://www.aclunc.org/blog/dac-vote-oakland-shows-how-surveillance-reform-begins-home.

[59] Herón Márquez Estrada, *This Time, Stanek Lands KingFish Phone Tracker*, Star Tribune, Mar. 23, 2010, http://www.startribune.com/this-time-stanek-lands-kingfish-phone-tracker/88977177/.

network that may be created by use of the device."[60] Similarly, in Illinois the legislature recently enacted a law requiring police to disclose to judges "a description of the nature and capabilities of the cell site simulator device that will be used and the manner and method of its deployment, including whether the cell site simulator device will obtain data from non-target communications devices."[61] Two recent California laws also address cell site simulators. Under the California Electronic Communications Privacy Act (CalECPA), all government entities must generally obtain a warrant to access electronic device information.[62] A second law requires that most local agencies obtain approval for the acquisition of a cell site simulator at a publicly noticed meeting, develop and implement a public use and privacy policy, and disclose agreements with other agencies.[63]

To address these concerns, the ACLU and EFF urge the Commission to adopt the recommendations contained at the end of this document, designed to ensure appropriate transparency, accountability, and oversight of state and local law enforcement's use of cell site simulator technology.

B. The FCC has enabled widespread use and concealment of cell site simulators, and should act immediately to conform state and local law enforcement's activities to the law.

Previous actions by the FCC have enabled both the widespread use of cell site simulators by state and local law enforcement agencies and the systematic concealment of that use, which has frustrated effective oversight. The Commission has an obligation to conform operation of cell site simulators to the requirements of the law and to remedy a problem that is,

[60] Wash. Rev. Code § 9.73.260(4)(c)(ii)(G).

[61] 725 Ill. Comp. Stat. 137/15(a)(1), as enacted by 2016 Ill. Legis. Serv. P.A. 99-622 (West).

[62] Cal. Penal Code § 1546.1.

[63] Cal. Gov. Code § 53166.

in significant part, of its own making. In granting equipment authorizations permitting the sale of cell site simulators to state and local law enforcement agencies, the FCC failed to impose any limitations on use that would have ensured compliance with the Communications Act and effectively ceded oversight to the FBI, an agency that has no expertise in or mandate to enforce that statute. The predictable result has been widespread violations of the Communications Act, as discussed *infra* Part II.

Two companies have applied for and received authorization from the FCC to manufacture and market cell site simulators within the United States: the Harris Corporation and Digital Receiver Technology (DRT).[64] Those companies' applications explicitly sought permission to sell the technology to state and local law enforcement agencies,[65] and at least one application, for Harris's "StingRay" device, was accompanied by letters to the FCC from various state and local law enforcement agencies stating their desire to purchase and use the equipment.[66] When the Commission granted equipment authorizations for the cell site

---

[64] *See* Aff. of William E. Chapman in Support of Respondent's Verified Answer, ¶ 7, *N.Y. Civil Liberties Union v. N.Y.C. Police Dep't*, No. 100788/2016 (N.Y. Sup. Ct., N.Y. Cty. Aug. 17, 2016), attached as Ex. A ("The United States has authorized two private companies (Digital Receiver Technology (DRT) and Harris Corporation) to manufacture this equipment."). Additional U.S. companies manufacture cell site simulator equipment, but have apparently not sought authorization to sell it to state and local law enforcement agencies in the United States. *See Government Cellphone Surveillance Catalogue*, The Intercept (Dec. 17, 2015), https://theintercept.com/document/2015/12/16/government-cellphone-surveillance-catalogue/.

[65] *See, e.g.*, Letter from Tania W. Hanna, Vice President, Legislative Affairs & Public Policy, Harris Corporation, to Marlene H. Dortch, Secretary, FCC, *Re: Final Request for Confidentiality of Harris Corporation for FCC ID No. NK73092523* (Apr. 28, 2011), https://apps.fcc.gov/oetcf/eas/reports/ViewExhibitReport.cfm?mode=Exhibits&RequestTimeout=500&calledFromFrame=N&application_id=9nDFvP9N200RJUhSYM6ASQ%3D%3D&fcc_id=NK73092523 (requesting that "[t]he marketing and sale of these devices shall be limited to federal/state/local public safety and law enforcement officials only").

[66] *See* Letter from Julius P. Knapp, Chief, FCC Office of Engineering & Tech., to Christopher Soghoian, Center for Applied Cybersecurity Research, Indiana University (Feb. 29, 2012), https://aclunc.org/sites/default/files/soghoian_fcc_foia.pdf (responding to FOIA request

simulators, it required that "[t]he marketing and sale of these devices shall be limited to federal, state, local public safety and law enforcement officials only," thus demonstrating that it understood the uses to which the technology would be put.[67]

As noted above, Harris expressly represented to the FCC that the "only" purpose of the equipment authorization was to give "state/local law enforcement officials with authority to utilize this equipment in emergency situations." Consistent with Harris' representation, the FCC could have, but did not, limit state and local agency use to "emergency situations" or include any other substantive limitations on state and local agency use that would have minimized interference with cellular communications or addressed unauthorized use of radio spectrum. Instead, the only requirement placed by the FCC on state and local law enforcement agencies in the equipment authorizations was a procedural one that requires those agencies to "advance coordinate with the FBI the acquisition and use of the equipment authorized under this authorization."[68] But the FBI does not have a mandate to regulate public spectrum in the public benefit.

---

and providing letters to the FCC from the Wisconsin Department of Justice, Houston Police Department, Alexandria, Virginia Police Department, and Anne Arundel County, Maryland Police Department).

[67] *See, e.g.*, FCC, Grant of Equipment Authorization, Harris Corporation, FCC Identifier NK73166210 (Mar. 2, 2012), https://apps.fcc.gov/oetcf/eas/reports/Eas731GrantForm.cfm?mode=COPY&RequestTimeout=500&application_id=S02SFOCotzKlbdYCDPFIlA%3D%3D&fcc_id=NK73166210; FCC, Grant of Equipment Authorization, Harris Corporation, FCC Identifier NK73092523 (Apr. 19, 2011), https://apps.fcc.gov/oetcf/eas/reports/Eas731GrantForm.cfm?mode=COPY&RequestTimeout=500&application_id=9nDFvP9N200RJUhSYM6ASQ%3D%3D&fcc_id=NK73092523.

[68] *Id.* The FBI requested this condition "in order to address concerns over the proliferation of surreptitious law enforcement surveillance equipment." *See* E-mail from [redacted] to [redacted], Re: grant condition(s) – RE: FCC response on Intended Operations (June 28, 2010, 10:56 EST), https://www.aclu.org/sites/default/files/assets/fcc_foia_harris_emails.pdf.

Perhaps predictably, the advance-coordination requirement has not ensured that state and local law enforcement's use of cell site simulators complies with the Communications Act, or otherwise resulted in any substantive oversight of the use of these devices by state and local law enforcement agencies. Rather, the FBI has used this requirement solely as an opportunity to impose an onerous non-disclosure agreement on state and local authorities. As the FBI explains,

> [t]his advance coordination is accomplished through and documented by a Non-Disclosure Agreement (NDA) executed between the state or local law enforcement agency and the FBI. Only upon execution of the NDA may a state or local agency purchase or otherwise acquire, use, or provide training about operating cell site simulator equipment from either of the two previously referenced companies. . . . Once the NDA is completed, the FBI notifies the manufacturer that the coordination has taken place.[69]

As a result of public records requests and litigation by civil liberties advocates and journalists, copies of the NDAs signed by two dozen state and local law enforcement agencies are now publicly available.[70] The terms of those NDAs are striking. Police departments are prohibited from disclosing "any information" about their acquisition and use of cell site simulators to the public or to "any other . . . government agency."[71] They are also required to withhold information from courts at all stages of judicial proceedings:

> The [police department] shall not, in any civil or criminal proceeding, use or provide any information concerning the Harris Corporation wireless collection

---

[69] Chapman Aff. ¶ 9, attached as Ex. A.

[70] *See Non-Disclosure Agreements Between FBI and Local Law Enforcement for Stingray*, Center for Human Rights & Privacy, http://www.cehrp.org/non-disclosure-agreements-between-fbi-and-local-law-enforcement/; *see also N.Y. Civil Liberties Union v. Erie Cty. Sheriff's Office*, 47 Misc.3d 1201(A), 2015 WL 1295966, at *11–12 (N.Y. Sup. Ct., Erie Cty., Mar. 17, 2015) (ordering release of NDA between the FBI and the Erie County Sheriff's Office pursuant to a Freedom of Information request from the New York Civil Liberties Union).

[71] Agreement between Federal Bureau of Investigation, Baltimore Police Department, and Office of the State's Attorney for Baltimore City, *Re: Purchase Wireless Collection Equipment/Technology and Non-Disclosure Obligations* (hereinafter "Baltimore NDA"), ¶¶ 3–4, 7 (executed Aug. 11, 2011), https://assets.documentcloud.org/documents/2290702/baltimore-pd-fbi-nda-13jul2011.pdf.

> equipment/technology . . . and any related documentation (including its technical/engineering description(s) and capabilities) beyond the evidentiary results obtained through the use of the equipment/technology including, but not limited to, during pre-trial matters, in search warrants and related affidavits, in discovery, in response to court ordered disclosure, in other affidavits, in grand jury hearings, in the State's case-in-chief, rebuttal, or on appeal, or in testimony in any phase of civil or criminal trial, without the prior written approval of the FBI.[72]

For years, these restrictions precluded public debate, judicial oversight, legislative regulation, and other accountability by keeping everyone outside of law enforcement in the dark. Police used the technology with impunity, while the privacy and integrity of Americans' cellular communications networks suffered.

The few courts that have recently learned of the use and concealment of cell site simulators have raised strong concerns. As the Maryland Court of Special Appeals wrote, "[w]e perceive the State's actions in this case to protect the Hailstorm technology, driven by a nondisclosure agreement to which it bound itself, as detrimental to its position and inimical to the constitutional principles we revere."[73] In a case now pending in the U.S. Court of Appeals for the Seventh Circuit, in which the Milwaukee Police Department used a cell site simulator but concealed it from judges and defense counsel as required by the FBI non-disclosure agreement,[74] a judge criticized the government for "completely conceal[ing]" information about its cell site simulator use and remarked that "there's a huge lack of candor on the government's

---

[72] *Id.* ¶ 5.

[73] *Andrews*, 134 A.3d at 339.

[74] *See* Agreement between Federal Bureau of Investigation and Milwaukee Police Department, *Re: Acquisition of Wireless Collection Equipment/Technology and Non-Disclosure Obligations* (executed Aug. 29, 2013), https://www.documentcloud.org/documents/2190206-milwaukee-pd-fbi-nda-13aug2013.html.

part that is very troubling."[75] A federal judge in Illinois has lamented that the secrecy caused by the NDA forces judges to search for basic information about cell site simulators on the internet and in law review and newspaper articles, rather than receiving it from the government itself.[76]

By giving the Harris Corporation and DRT carte blanche to sell cell site simulators to local law enforcement agencies without imposing a licensing structure governing the use of the equipment, and by providing the FBI with the means to impose a rigid secrecy regime on those agencies, the FCC has enabled violations of the Communications Act and has stymied oversight efforts. Any response to the pending Complaint and Petition must be designed to remedy the problems of excessive secrecy and illegal use of the technology.

II. The Use of Cell Site Simulators by State and Local Law Enforcement Agencies Violates Sections 301 and 333 of the Communications Act

As explained in the Complaint and Petition, the use of cell site simulators by the Baltimore Police Department and other state and local law enforcement agencies violates the Communications Act.[77]

Section 333 of the Communications Act provides that "[n]o person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this chapter."[78] Cell site simulators "interfere with or cause interference to" cellular communications in at least two ways. First, by "transmitting as a cell

---

[75] Oral Argument, *United States v. Patrick*, No. 15-2443 (7th Cir. May 24, 2016) (statement of Wood, C.J.), http://media.ca7.uscourts.gov/sound/external/nr.15-2443.15-2443_05_24_2016.mp3.

[76] *In re Application of the U.S. for an Order Relating to Telephones Used by Suppressed*, No. 15 M 0021, 2015 WL 6871289, at *1 (N.D. Ill. Nov. 9, 2015).

[77] *See* Complaint at 30–33.

[78] 47 U.S.C. § 333.

tower" and causing cellular phones in the area "to transmit signals to the simulator . . . in the same way that they would with a networked tower," cell site simulators can cause "the target cellular device (*e.g.*, cell phone) and other cellular devices in the area [to] experience a temporary disruption of service from the service provider."[79] As a police sergeant with the Metropolitan Police Department in Washington, D.C., explained in court testimony, "[o]nce [the cell site simulator] grabs [the phone] and holds on to it for a minute, it cannot contact immediately with an actual [cellular] tower."[80]

Second, some cell site simulator models interfere with phones' communications on the 3G and 4G cellular networks in order to force the phones to communicate over the significantly less secure 2G network, which is vulnerable to spoofing with a cell site simulator:

> One of the primary ways that stingrays operate is by taking advantage of a design feature in any phone available today. When 3G or 4G networks are unavailable, the handset will drop down to the older 2G network. While normally that works as a nice last-resort backup to provide service, 2G networks are notoriously insecure. Handsets operating on 2G will readily accept communication from another device purporting to be a valid cell tower, like a stingray. So the stingray takes advantage of this feature by jamming the 3G and 4G signals, forcing the phone to use a 2G signal.[81]

---

[79] Dep't of Justice, *Policy Guidance: Use of Cell-Site Simulator Technology*, at 2, 5 (Sept. 3, 2015), https://www.justice.gov/opa/file/767321/download.

[80] Motions Hr'g Transcript at 44, *United States v. Jones*, No. 2013-CF1-18140 (D.C. Super. Ct. Oct. 17, 2014), *appeal pending*, No. 15-CF-322 (D.C.).

[81] Cyrus Farivar, *Cities Scramble to Upgrade "Stingray" Tracking as End of 2G Network Looms*, Ars Technica, Sept. 1, 2014, http://arstechnica.com/tech-policy/2014/09/cities-scramble-to-upgrade-stingray-tracking-as-end-of-2g-network-looms/. This type of interference is possible because

> [m]ore recent cellular phone systems, including so-called 3G and 4G networks, now include the capability for phones to authenticate the network base stations. However, even the latest smartphones are backward compatible with older, vulnerable phone network technologies, which allows the phone to function if it is taken to a rural location or foreign country where the only service offered is 2G.

"Indeed, many of the manufacturers of [cell site simulator equipment] openly advertise the ability to jam 3G and 4G networks in order to force telephones to connect an active interception device masquerading as a 2G base station."[82] Jamming phones' ability to connect to legitimate 3G and 4G networks forces them to make a 2G connection to a device that is not actually part of the cellular network (the cell site simulator). That, in turn, prevents the phones from being able to make and receive calls, send and receive text messages, and use internet data service. Although native 4G/LTE cell site simulators such as the Hailstorm device purchased by the Baltimore Police Department and some other law enforcement agencies[83] likely do not require that 3G/4G service be jammed,[84] many law enforcement agencies still possess the far more disruptive 2G Stingrays that they have used for a number of years.[85]

> As a result, modern phones remain vulnerable to active surveillance via a *protocol rollback* attack in which the nearby 3G and 4G network signals are first jammed.

Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 Harv. J.L. & Tech. 1, 12 n.52 (2014) (citations omitted).

[82] Pell & Soghoian, 28 Harv. J.L. & Tech. at 70 (citing, *inter alia*, *3G-GSM Tactical Interception & Target Location*, Gamma Group, at 40 (2011), *available at* http://info.publicintelligence.net/Gamma-GSM.pdf ("This device will emulate a 3G network to attract 3G mobiles and, for designated Targets, selectively push them to GSM where they remain unless they are rebooted or pushed back to 3G by the GSM system.")).

[83] *See State v. Andrews*, 134 A.3d 324, 329 (Md. Ct. Spec. App. 2016) (discussing Baltimore Police Department's use of "a cell site simulator known by the brand name 'Hailstorm'"); Harris Corporation, Invoice No. INV6779-04018 (Jan. 15, 2014), https://www.aclu.org/legal-document/wilmington-nc-police-department-invoice-stingray-ii-hailstorm-upgrade (invoice to Wilmington, N.C., Police Department for "StingRay II to HailStorm Upgrade"); Harris Corporation, Quotation No. QTE6779-04207 (Mar. 13, 2013), https://www.aclu.org/sites/default/files/field_document/sunrise_fl_-_harris_corp_quotation_130313.pdf (price quotation for Sunrise, Florida, Police Department listing Stingray II-to-Hailstorm upgrade).

[84] *See* Internal Revenue Service, Privacy Impact Assessment for CI Use of Stingray II, PIA ID Number 1832, at 2 (July 29, 2016), https://www.irs.gov/pub/irs-utl/stingrayII-pia.pdf ("The

As the FCC has made clear, operation of devices that "block, jam, or otherwise interfere with authorized radio communications" violates the Communications Act and is not permitted, including by state and local law enforcement agencies.[86] Any enforcement action against the Baltimore Police Department and any enforcement advisory issued to other state and local law enforcement agencies must make clear that use of cell site simulators violates Section 333's prohibition on interference with cellular communications.

Use of cell site simulators by state and local law enforcement agencies also violates Section 301 of the Communications Act, which provides that "[n]o person shall use or operate any apparatus for the transmission of energy or communications or signals by radio . . . except under and in accordance with this chapter and with a license in that behalf granted under the provisions of this chapter."[87] A radio spectrum license is distinct from the equipment authorization granted for the broadcast device itself. Just as cellular service providers must use base station equipment covered by an equipment authorization[88] *and* must obtain a separate

---

Hailstorm upgrade provides an additional two channels of monitoring that allows IRS-CI to target 4G phones/LTE devices.").

[85] *See, e.g.*, John Dodge, *After Denials, Chicago Police Department Admits Purchase Of Cell-Phone Spying Devices*, CBS Chicago, Oct. 1, 2014, http://chicago.cbslocal.com/2014/10/01/chicago-police-department-admits-purchase-of-cell-phone-spying-devices/ (showing Chicago Police Department document listing "StingRay II – Upgrade"); County of Erie, New York, Purchase Order No. 4600005905 (Dec. 12, 2008), http://www.nyclu.org/files/Purchase-Orders.pdf (listing purchase of "KingFish" and "StingRay" systems from Harris Corporation).

[86] *FCC Enforcement Advisory, Warning: Jammer Use is Prohibited*, DA 14-1785, Public Notice, 29 FCC Rcd 14737 (2014), https://apps.fcc.gov/edocs_public/attachmatch/DA-14-1785A1_Rcd.pdf.

[87] 47 U.S.C. § 301.

[88] *See, e.g.*, FCC, Grant of Equipment Authorization, Nokia Solutions and Networks, FCC Identifier VBNFXCB-01 (June 27, 2016), https://apps.fcc.gov/oetcf/tcb/reports/Tcb731GrantForm.cfm?mode=COPY&RequestTimeout=5

broadcast license to operate it,[89] state and local law enforcement agencies must be properly licensed by the FCC to use cell site simulators, even when the simulators themselves are the subject of equipment authorizations. Because cell site simulators broadcast on licensed portions of the radio spectrum,[90] their operation by state and local authorities requires a cellular spectrum license. Indeed, at least one private company has received an experimental radio service license[91] from the FCC for operation of cell site simulator devices "in accordance with [a specific] program of experimentation," further confirming that a license is needed for cell site simulator use.[92]

It does not appear that the Baltimore Police Department or other state and local law enforcement agencies have obtained licenses to operate cell site simulators.[93] Nor is it clear that there is any mechanism through which they could do so under current FCC regulations. The governing regulations provide that "Stations in the Wireless Radio Services must be used and operated only in accordance . . . with a valid authorization granted by the Commission under the

---

00&tcb_code=&application_id=W%2BhGwDvydKI7h4%2FSk9ER%2BQ%3D%3D&fcc_id=VBNFXCB-01 (equipment authorization for "Cellular Base Station").

[89] *See, e.g.*, PCS Broadband License - WPZQ943 - T-Mobile License LLC (Dec. 10, 2014), available at http://wireless2.fcc.gov/UlsApp/UlsSearch/license.jsp?licKey=2596021.

[90] *See* Complaint at 11.

[91] Experimental radio service licenses are issued pursuant to Part 5 of the FCC's rules. *See* 47 C.F.R. § 5.53.

[92] FCC Experimental Radio Station Construction Permit & License, File No. 0145-EX-PL-2011 (effective Aug. 30, 2011), https://apps.fcc.gov/els/GetAtt.html?id=118884&x=.; Application for New or Modified Radio Station Under Part 5 of FCC Rules – Experimental Radio Service (Other Than Broadcast), File No. 0145-EX-PL-2011 (Mar. 21, 2011), https://apps.fcc.gov/oetcf/els/reports/442_Print.cfm?mode=current&application_seq=47486&license_seq=48001 (application from Phoenix Global Support for experimental use license to operate "Stingray" and "Stingray-II" devices, among other technology).

[93] *See* Complaint at 12.

provisions of this part."[94] Although state or local police departments operating a cell site simulator meet the definition of "radio station" under the regulations,[95] they are arguably neither "Stations in the Wireless Radio Services"[96] nor are they eligible to receive an "authorization" as defined.[97] Continued use of cell site simulators by state and local agencies is illegal under Section 301 of the Communications Act, and will remain so until and unless the Commission creates an appropriate procedure for issuing licenses to those agencies. The Commission may wish to consider issuing a notice of inquiry to solicit public input and engaging in a rulemaking process to this end.

Because use of cell site simulators by state and local law enforcement agencies violates the Communications Act, the FCC should issue an enforcement advisory ordering such uses to cease. There should be immediate cessation of operation of cell site simulators by state and local law enforcement agencies, at least until a proper licensing procedure that provides for necessary oversight is put in place. Such an enforcement order would not unduly impact public safety. Law

---

[94] 47 C.F.R. § 1.903(a).

[95] 47 C.F.R. § 1.907 ("*Radio station.* A separate transmitter or a group of transmitters under simultaneous common control, including the accessory equipment required for carrying on a radio communications service.").

[96] "Wireless Radio Services" is defined as "[a]ll radio services authorized in parts 13, 20, 22, 24, 26, 27, 74, 80, 87, 90, 95, 96, 97 and 101 of this chapter, whether commercial or private in nature." 47 C.F.R. § 1.907. None of the enumerated parts of Chapter 47 appear to contemplate the grant of a spectrum broadcast license to a state or local law enforcement agency operating a cell site simulator on licensed portions of the spectrum.

[97] As defined in the regulations, an "authorization" under 47 C.F.R. § 1.903 can be issued only to "a station in the Wireless Telecommunications Services." 47 C.F.R. § 1.907. "Wireless Telecommunications Services" is defined in § 1.907 with reference to the definition of "telecommunications service" in 47 U.S.C. § 153, which is "the offering of telecommunications for a fee directly to the public." 47 U.S.C. § 153(53). State and local law enforcement agencies operating cell site simulators are not "offering . . . telecommunications for a fee directly to the public." In fact, they are interfering with "the offering of telecommunications for a fee directly to the public."

enforcement agencies can continue to be able to obtain precise, real-time cell phone location information from service providers pursuant to a properly issued judicial warrant or the invocation of an emergency.[98] That capability is a result of the FCC's own rules, adopted in 1996 and implemented by 2001, that require cellular service providers to have "the capability to identify the latitude and longitude of a mobile unit making a 911 call."[99] Service providers can engage that capability not only in response to 911 calls, but also in response to properly issued law enforcement requests.[100] Indeed, law enforcement agencies obtain real-time cell phone location information from service providers tens of thousands of times each year.[101] Moreover, although service providers cannot always locate phones with the same precision as cell site simulators, the precision and accuracy of this mandated cell phone location capability will be increasing. In January 2015, the FCC adopted new rules to improve law enforcement's ability to

---

[98] *See, e.g.*, *United States v. Caraballo*, __ F.3d __, 2016 WL 4073248, at *2-3 (2d Cir. Aug. 1, 2006) (describing how the officers were able to discover GPS location of a person from Sprint in an exigent circumstance); *Tracey v. State*, 152 So.3d 504 (Fla. 2014) (requiring warrant under Fourth Amendment for real-time cell phone location requests to service providers); *State v. Earls*, 70 A.3d 630 (N.J. 2013) (same, under New Jersey Constitution).

[99] *See* Report and Order and Further Notice of Proposed Rulemaking, *In re Revision of the Comm'n's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Sys.*, 11 F.C.C. Rcd. 18676, 18683–84 (1996).

[100] *See, e.g.*, AT&T, *Transparency Report*, at 7 (July 2016), http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_TransparencyReport_July2016.pdf (discussing law enforcement demands for "precise GPS coordinates of the device"); Sprint Corporation, *Transparency Report*, at 3 (July 2016), http://goodworks.sprint.com/content/1022/files/Transaparency%20Report%20July2016.pdf ("Sprint receives court orders requiring the provision of information regarding real-time location of a customer device on the Sprint network.").

[101] AT&T, *Transparency Report*, *supra*, at 4 (listing 16,547 real-time location demands from July 2015 through June 2016); Sprint, *Transparency Report*, *supra*, at 4 (listing 62,966 real-time location requests from July 2015 through June 2016).

identify the location of callers when they are indoors,[102] and require service providers to develop techniques to determine the altitude of the phone, and thus which floor of a building it is located on.[103]

Federal agencies also currently possess the technology, including the FBI, U.S. Marshals Service, Secret Service, Drug Enforcement Administration, Bureau of Alcohol, Tobacco, Firearms, and Explosives, Immigration and Customs Enforcement, and even the Internal Revenue Service.[104] Federal law enforcement agencies are generally not constrained by many of the licensing requirements applicable to other entities,[105] but federal use, including any use in "support of . . . State and Local law enforcement agencies," must currently comply with the Department of Justice and Department of Homeland Security guidelines for cell site simulators.[106] Although FCC regulation of federal use of cell site simulators is beyond the scope

---

[102] *In re Wireless E911 Location Accuracy Requirements*, PS Docket No. 07-114, Fourth Report and Order at 1 (FCC Jan. 29, 2015) [Wireless E911 Order], available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-9A1.pdf; David Schneider, *New Indoor Navigation Technologies Work Where GPS Can't*, IEEE Spectrum (Nov. 20, 2013), http://spectrum.ieee.org/telecom/wireless/new-indoor-navigation-technologies-work-where-gps-cant.

[103] Wireless E911 Order at 3–4.

[104] *See Stingray Tracking Devices: Who's Got Them?*, ACLU, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (listing federal law enforcement agencies known to possess cell site simulators).

[105] 47 U.S.C. §§ 302a(c), 305(a), 323.

[106] Dep't of Justice, *Policy Guidance: Use of Cell-Site Simulator Technology*, *supra*, at 6 ("This policy applies to all instances in which Department components use cell-site simulators in support of . . . State and Local law enforcement agencies."); Dep't of Homeland Sec., Department Policy Regarding the Use of Cell-Site Simulator Technology, Policy Directive 047-02, at 8 (Oct. 19, 2015), https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf ("This policy applies to all instances in which [DHS] Components use cell-site simulators in support of . . . state and local law enforcement agencies.").

of this filing, the Commission should consider any available steps it can take to minimize interference with cellular communications caused by federally operated cell site simulators, and to prevent state and local law enforcement agencies from circumventing local democratic oversight mechanisms and transparency requirements by soliciting assistance from federal law enforcement agencies rather than seeking to use their own cell site simulator equipment in accordance with applicable protections and limitations.

III. Any System for Granting Cell Site Simulator Use Licenses to State and Local Law Enforcement Agencies Must Be Predicated on Strong Transparency, Accountability, and Oversight to Protect Against Abuse.

Any grant of a broadcast license to a state or local law enforcement agency must be predicated on strong protections to minimize interference with cellular communications and to facilitate proper oversight.[107] The following proposed requirements are intended to end the corrosive secrecy that has frustrated attempts to regulate cell site simulator use and to protect the integrity and privacy of America's cellular communications networks. This list is not exclusive, and the Commission should solicit additional public input, including by considering issuing a notice of inquiry and engaging in a rulemaking process, as it decides how to appropriately regulate the technology. Until and unless a licensing scheme including such protections is put in place, the Commission should order state and local agencies to cease their operation of cell site simulators.

---

[107] Any scheme that permitted state and local law enforcement agencies to use cell site simulators pursuant to the consent and approval of the service providers that hold the broadcast licenses for the relevant portions of the cellular spectrum would need to include equivalent protections, including public reporting of the number of law enforcement requests and service provider approvals. In addition, the FCC should consider the extent to which any such approvals trigger the protections of the Communications Assistance for Law Enforcement Act, which provides that "information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . shall not include any information that may disclose the physical location of the subscriber." 47 U.S.C. § 1002(a).

1. Public Debate and Local Legislative Oversight.

Before a local law enforcement agency can obtain or operate a cell site simulator, there should be public debate and local legislative oversight to ensure that the right questions are asked and answered about the cell site simulator and that any use would safeguard civil rights.

- *Express and Specific Local Legislative Authorization*

The relevant local elected legislative body (*i.e.*, city council, county board of supervisors, etc.) must grant explicit authorization to acquire or use the technology. That authorization must be obtained by the law enforcement agency under procedures for public notice and debate.

- *Informed Public Debate—Surveillance Impact Report and Proposed Use Policy*

In seeking legislative approval, a law enforcement agency should be required to prepare and submit several resources to help facilitate an informed public debate: (1) a report on how the cell site simulator works: (2) a surveillance impact report; and (3) a proposed use policy The surveillance impact report, at a minimum, should disclose the cell site simulators' impact on cellular communications, on the privacy of third parties, and on civil rights, including an analysis of any racially disparate impact that law enforcement's use of cell site simulators may or will have. A surveillance impact assessment that specifically analyzes the civil rights impact is crucial because many of the law enforcement agencies that are known to operate cell site simulators have a documented record of racial bias in their policing activities.[108] The proposed Use Policy should, at a minimum, detail: purpose and authorized use; data collection, access,

[108] *See supra* note 24.

protection, and retention; public access and third party sharing; and training and auditing and oversight mechanisms.

- *Ongoing Oversight and Accountability*

If a cell site simulator is approved for purchase or use, there must be ongoing oversight and accountability through enforcement mechanisms and annual reporting and review by local lawmakers to make sure that policies are being followed and civil rights are being safeguarded.

2. Judicial Oversight.

Before a state or local law enforcement agency may use a cell site simulator in any investigation, it must fully and accurately disclose to a judge in a warrant application information about the nature and capabilities of the technology and how it will interfere with cellular communications.[109] The warrant application must include proposed procedures for minimizing the cell site simulator's impact on third parties' communications, as well as procedures for providing notice to persons who are tracked or located using the cell site simulator.

3. Compliance with Department of Justice Policy Guidance

State and local law enforcement agencies must comply with the Department of Justice policy guidance on use of cell site simulators, which mandates disclosure to courts of information about interference with cellular communications and other harms caused by the technology, among other protections.[110] State and local law enforcement agencies should be

---

[109] Under the Fourth Amendment, a warrant is not required when there are exigent circumstances.

[110] *See* Dep't of Justice, *Policy Guidance: Use of Cell-Site Simulator Technology*, *supra*.

permitted to adopt more protective or stringent cell site simulator policies; the terms of the Department of Justice policy guidance are a floor, not a ceiling.

4. Minimization Procedures

State and local law enforcement agencies should also adopt procedures for the use of cell site simulators that minimize the impact on third parties' cellular communications. These could include such measures as reducing the broadcast range of the device,[111] limiting the time it can be operated (for example, that it be operated "no longer than 3 minutes at a time, with a rest period of at least 2 minutes between each use"),[112] and using a directional antenna to focus the signals on the area where the target is believed to be.[113]

5. Annual Reporting

State and local law enforcement agencies should annually report to the FCC information about which and how many cell site simulators they have purchased and used, the number of times they used the technology, the types of crimes they have used the technology to investigate, the locations in which they used the technology, and best estimates of the number of third parties' phones affected. The FCC should annually publish a report containing this information.

6. Public Registry of Cell Site Simulator Devices and Usage Policies

---

[111] Colin Freeze, *RCMP Listening Device Capable of Knocking Out 911 Calls, Memo Reveals*, Globe & Mail, Apr. 18, 2016, http://www.theglobeandmail.com/news/national/rcmp-listening-tool-capable-of-knocking-out-911-calls-memo-reveals/article29672075/ (discussing cell site simulator procedures used by Royal Canadian Mounted Police to minimize interference with cellular communications).

[112] *Id.*

[113] *In re Application of the U.S. for an Order Relating to Telephones Used by Suppressed*, No. 15 M 0021, 2015 WL 6871289, at *3 (N.D. Ill. Nov. 9, 2015).

The FCC should create a public registry of cell site simulator devices and usage policies. Any state or local law enforcement agency that possesses a cell site simulator should report to a publicly available FCC registry the trade name of the device, the FCC-assigned identifier of the device ("FCC ID"), and the use policy that will govern use of the device by that agency.

7. Compliance with FCC Licenses

A wireless carrier may only authorize a state or local law enforcement agency to use radio spectrum for which it has a license, if doing so is consistent with the carrier's license, and must annually notify the FCC in a publicly available report the list of all state or local law enforcement agencies that sought to use its radio spectrum, and for each request by a state or local law enforcement agency to use the carrier's spectrum: the type of legal authorization obtained by the state or local law enforcement agency for use of the cell site simulator, the criminal law alleged to be violated, and whether the carrier authorized use of its spectrum.

Conclusion

For the foregoing reasons, the ACLU and EFF urge the Commission to grant the relief requested in the Complaint and Petition by (1) initiating an enforcement action against the Baltimore Police Department for using cell site simulators in violation of the Communications Act, (2) issuing an enforcement advisory informing other state and local law enforcement agencies that they must cease using cell site simulators, at least until an appropriate licensing system is put in place by the FCC, and (3) ensuring that any licensing scheme applicable to state and local agencies seeking to use cell site simulators is predicated on strong protections to

minimize interference with cellular communications and to facilitate proper transparency, accountability, and oversight.

September 1, 2016

Respectfully Submitted,

/s/ Nathan Freed Wessler

Nathan Freed Wessler
Christopher Soghoian
Speech, Privacy, and Technology Project
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad St., 18th Fl.
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

Karin Johanson
Neema Singh Guliani
Washington Legislative Office
AMERICAN CIVIL LIBERTIES UNION
915 15th St., NW, 6th Fl.
Washington, DC 20005
(202) 544-1681

Linda Lye
Nicole A. Ozer
Matt Cagle
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm St.
San Francisco, CA 94111
(415) 621-2493

Mariko Hirose
NEW YORK CIVIL LIBERTIES UNION FOUNDATION
125 Broad St., 19th Fl.
New York, NY 10004
(212) 607-3300

David Rocah
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF MARYLAND
3600 Clipper Mill Road
Suite 350
Baltimore, MD 21211
(410) 889-8550

Jennifer Lynch
Lee Tien
Ernesto Falcon
ELECTRONIC FRONTIER FOUNDATION
815 Eddy St.
San Francisco, CA 94109
(415) 436-9333

EXHIBIT A

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

---------- x

NEW YORK CIVIL LIBERTIES UNION,

Petitioner,

-against-

THE NEW YORK CITY POLICE DEPARTMENT,

Respondent.

---------- x

AFFIDAVIT OF WILLIAM E. CHAPMAN IN SUPPORT OF RESPONDENT'S VERIFIED ANSWER

Index No. 100788/2016
I.A.S. Part 17
(Hagler, J.)

STATE OF NEW YORK)
) SS:
COUNTY OF NEW YORK)

I, William E. Chapman, depose and say as follows:

1. I am a Program Manager (PM) and Information Technology Specialist with the Federal Bureau of Investigation (FBI). I am assigned to the Tracking Technology Unit (TTU), Technical Surveillance Section (TSS), Operational Technology Division (OTD) of the FBI in Quantico, Virginia, which has oversight responsibility for the FBI's cell-site simulator (CSS) program. I have been employed by the FBI since 1999. TTU is the responsible unit for the procurement and deployment of technical assets and capabilities to covertly locate and identify cellular devices used by targets of interest in support of all FBI investigative, intelligence collection and operational programs. As such, TTU personnel are responsible for overseeing the FBI's use of CSS equipment to locate and/or identify cellular devices, as well as for setting policy and procedures governing the use of FBI CSS equipment, for monitoring compliance with FBI policy in these areas, and for assessing whether information pertaining to

CSS equipment, technology or tradecraft is law enforcement sensitive (LES) in accordance with FBI policy on LES information.

2. Because of the nature of my official duties, I am familiar with FBI policy concerning cell site simulators . The statements contained in this affidavit are based upon my personal knowledge, upon information provided to me in my official capacity, and upon conclusions and determinations reached and made in accordance therewith.

Summary

BACKGROUND INFORMATION ABOUT CELL SITE SIMULATORS AND THE FEDERAL GOVERNMENT SHARING THE TECHNOLOGY WITH STATE AND LOCAL LAW ENFORCEMENT PARTNERS

3. Cell site simulator technology provides valuable assistance in support of important public safety objectives. Whether deployed as part of a fugitive apprehension effort, a complex narcotics investigation, or to locate or rescue a kidnapped child, cell site simulators fulfill critical operational needs. Cell-site simulator technology is also an important tool in the Federal Government's efforts to protect and defend the United States against terrorist and other threats to our national security. Indeed, cell site simulators are defense articles on the U.S. Munitions List and thus are prohibited from export under the International Traffic In Arms Regulations (ITAR) without a license from the Department of State. *See* 22 C.F.R. §§ 120.1 – 130.17 (ITAR); 22 C.F.R. § 121.1, U.S. Munitions List Category XI(b).[1] Moreover, technical data about Category XI(b) defense articles, including cell site simulators, is also regulated and cannot be exported without a license pursuant to 22 C.F.R. § 121.1, Category XI(d). Technical

[1] Effective December 29, 2015, Category XI(b) consists of "[e]lectronic systems or equipment … specially designed for intelligence purposes that collect, survey, monitor, or exploit the electromagnetic spectrum (regardless of transmission medium), or for counteracting such activities." 80 Fed. Reg. 37975-76 (Jul. 2, 2015).

data is "[i]nformation ... which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles." 22 C.F.R. § 120.10(a)(1).

4. Law enforcement agents can use cell site simulators to help locate cellular devices whose unique identifiers are already known to law enforcement, or to determine the unique identifiers of an unknown device by collecting limited signaling information from devices in the simulator operator's vicinity. This technology is one tool among many traditional law enforcement techniques available to law enforcement.

5. In general, cell site simulators function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the device identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would with a networked tower.

6. A cell site simulator receives and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider. When used to locate a known cellular device, a cell site simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the cell site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone. When used to identify an unknown device, the cell site simulator obtains signaling information from non-target devices in the target's vicinity for the limited purpose of distinguishing the target device.

7. By transmitting as a cell tower, cell site simulators acquire the identifying information from cellular devices. Cell site simulator/pen register technology was originally developed under contract with the Federal Government. The United States has authorized two

private companies (Digital Receiver Technology (DRT) and Harris Corporation) to manufacture this equipment and since 2010 has expressly conditioned their ability to sell the equipment to state and local law enforcement agencies on specific and controlled terms reflecting its sensitive nature, as explained in the following paragraphs.

8. Federal law prohibits the use of any radio transmission equipment, except as authorized by the Federal Communications Commission (FCC). Cell site simulator equipment is radio transmission equipment. The FCC has issued authorization for manufacturers to sell their equipment to state and local law enforcement agencies with two conditions: (1) the marketing and sale of cell site simulator devices is limited to Federal, state, and local public safety and law enforcement agencies; and (2) state and local agencies must coordinate with the FBI in advance of their acquisition and use of the equipment. *See* Exhibit A hereto (FCC Grant of Equipment Authorization to Harris Corp., dated March 2, 2012).

9. This advance coordination is accomplished through and documented by a Non-Disclosure Agreement (NDA) executed between the state or local law enforcement agency and the FBI. Only upon execution of the NDA may a state or local agency purchase or otherwise acquire, use, or provide training about operating cell site simulator equipment from either of the two previously-referenced companies. Thus, when a state or local law enforcement agency contacts one of these manufacturers about purchasing such equipment, the manufacturer notifies the FBI about the agency's interest. The FBI then contacts the agency to begin the coordination process, including the NDA. Once the NDA is completed, the FBI notifies the manufacturer that the coordination has taken place.

10. Some state and local law enforcement agencies acquired cell site simulator equipment before institution of the requirement to coordinate and execute NDAs with the FBI.

See, e.g., *Hodai v. City of Tucson*, 239 Ariz. 34, 365 P.3d 959 (Ariz. Ct. App. 2016). The New York City Police Department (NYPD) first acquired cell site simulator equipment from Harris Corporation prior to institution of the coordination and NDA requirements. Its subsequent acquisition of cell site simulator equipment from Harris Corporation was covered by the NDA. The fact that an NDA was not in place for its initial purchase does not mean there was no Federal interest in the technology and equipment. Indeed, as indicated above, the NDA requirement simply formalized and documented that interest.

11. Through the NDAs, state and local law enforcement agencies stipulate that they will not disclose information about the technology and equipment and that they will notify the FBI upon receipt of any request for such information to provide the Federal Government the opportunity to protect the important Federal equities at stake.

12. The NYPD signed an NDA with the FBI as a prerequisite to purchasing cell site simulator systems from Harris Corp. in June of 2011. The NDA between the FBI and NYPD provides, in part:

> Disclosing the existence of and the capabilities provided by [cell site simulator equipment and technology] to the public would reveal sensitive technological capabilities possessed by the law enforcement community and may allow individuals who are the subject of investigation wherein this equipment/technology is used to employ countermeasures to avoid detection by law enforcement. This would not only potentially endanger the lives and physical safety of law enforcement officers and other individuals, but also adversely impact criminal and national security investigations. That is, disclosure of this information could result in the FBI's inability to protect the public from terrorism and other criminal activity because, through public disclosures, this technology has been rendered essentially useless for future investigations. In order to ensure that [cell site simulator equipment and technology] continues to be available for use by the law enforcement community, the equipment/technology and any information related to its functions, operation, and use shall be protected from potential compromise by precluding disclosure of this information to the public . . . .

13. In addition, by executing the NDA, NYPD agreed that it "will not distribute, disseminate, or otherwise disclose any information concerning the wireless collection equipment/technology or any software, operating manuals, or related technical documentation (including its technical/engineering descriptions(s) and capabilities) to the public, including to any non-law enforcement individuals or agencies," and that "[i]n the event that [the NYPD] receives a request pursuant to the Freedom of Information Act (5 U.S.C. § 552) or an equivalent state or local law, the civil or criminal discovery process, or other judicial, legislative, or administrative process, to disclose information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities), the [NYPD] will immediately notify the FBI . . . in order to allow sufficient time for the FBI to seek to prevent disclosure through appropriate channels."

PETITIONER'S FOIL REQUEST

14. In this case, Petitioner, the NYCLU, requested records under the New York Public Officers Law on April 13, 2015. Petitioner sought records about NYPD's use of cell site simulators, including, *inter alia*, purchase orders, contracts and agreements that contain the types and number of cell site simulators owned or used by NYPD; technical specifications of the equipment; policies, guidelines, or training on use of the equipment; the type of information collected by the equipment; and cases in which the equipment was used. NYPD granted the request in part, providing access to a redacted NDA with Harris Corporation and several pages of data listing deployment of cell site simulators, and denied the remainder of the request. After an administrative appeal, NYPD affirmed its prior response and provided a detailed explanation as to the exemptions invoked.

15. Petitioner filed this lawsuit on May 9, 2016.

16. NYPD brought the lawsuit to the FBI's attention consistent with its obligations under its NDA. The FBI seeks to protect two categories of information: (1) technical specifications and capabilities of cell site simulator systems and (2) makes and models of cell site simulator systems which it is the FBI's understanding is contained in the records at issue.

17. The information protected within Category 1 above—technical specifications and capabilities of cell site simulator systems—includes information about capabilities of (then) existing equipment and capabilities sought through upgrades of equipment; platforms and modes on which the equipment can be operated; functionality; limitations; descriptions of equipment installations; technical specifications of equipment; and information about/descriptions of particular configurations of the equipment.

18. The information protected within Category 2 in this case—makes and models of cell site simulator systems—includes the names and models of cell site simulator systems and the components necessary to configure the systems in various ways.

19. The FBI has assessed that disclosure of these categories of information to the public would pose significant risks to effective law enforcement, and ultimately to the safety of the public and the national security of the United States. Accordingly, the FBI concluded that these categories of information need to be protected in furtherance of public safety and national security.

RISK OF HARM FROM DISCLOSURE

20. The Federal Government, including but not limited to the FBI, has a strong interest in protecting from disclosure technical and operational information about cell-site simulators and their use. Accordingly, the FBI protects information about this equipment and

associated techniques from disclosure. The FBI directs its agents that, while the product of an identification or location operation may be disclosed (*e.g.*, that a suspect was apprehended or a victim recovered at a particular location), neither the details of the equipment's operation nor the tradecraft involved in its use may be disclosed. In the federal Freedom of Information Act (FOIA) context, the FBI protects such information pursuant to FOIA Exemption 7(E), 5 U.S.C. § 552(b)(7)(E). Additionally, the Federal Government asserts the law enforcement privilege in discovery to shield such information, because disclosure would allow criminal defendants and others to ascertain law enforcement's capabilities and limitations in this area, and thus to develop countermeasures. *See, e.g., U.S. v. Rigmaiden*, 844 F. Supp. 2d 982 (D. Ariz. 2012) (federal criminal prosecution); *U.S. v. Garey*, 2004 WL 2663023 (M.D. Ga. Nov. 15, 2004) (same). *Cf. California v. Michaels*, Case No. 5-140709-7 (Cal. Super. Ct., Contra Costa County) (Orders dated Nov. 4, 2015 and Dec. 3, 2015) (state criminal prosecution applying "official information" privilege under California Evidence Code § 1040 to cell site simulator information based on testimony by FBI Supervisory Special Agent). It is just as imperative for this information to be protected in response to requests under state information access statutes.

21. In particular, cell site simulator equipment is a key tool in the investigation, interdiction, and suppression of criminal and terrorist activity and threats to the national security of the United States. Disclosure of even minor details about cell site simulators may cause harm to law enforcement efforts and the national security of the United States because, much like a jigsaw puzzle, each detail may aid in piecing together other bits of information even when the individual piece is not of obvious importance itself. Thus, disclosure of what appears to be innocuous information about cell site simulators may provide adversaries (criminals and terrorists alike) with information about the capabilities, limitations, and circumstances of the

equipment's use, and would allow such adversaries to accumulate information and draw conclusions about the use and technical capabilities of the technology. In turn, this would provide them with the information necessary to develop defensive technology, modify their behaviors, and otherwise take countermeasures designed to thwart the use of the technology in order to evade detection by law enforcement and circumvent the law. Adversaries and others could also use such information to disrupt and dismantle the functioning of the equipment altogether, thus rendering it nonfunctional and obviating its utility in any circumstances. Indeed, Internet bloggers are already outlining ways to try to circumvent the Federal Government's cellular locating and identifying capabilities. Rendering this technology obsolete would seriously undermine the criminal law enforcement efforts of Federal, state, and local law enforcement agencies nationwide, as well as the efforts of the Federal Government to protect and safeguard the national security of the United States.

22. NYPD identified responsive information in various records related to procurement, purchasing, and contracting. As mentioned above, the FBI asked NYPD to protect the above categories of information found in these records. The risk of harm from disclosing each category of information, on its own or in combination with other information, is discussed below.[2]

---

[2] Although some of the information at issue here concerns older equipment (*i.e.*, the DRT equipment), disclosure of technical, tradecraft, and made/model information could nevertheless prejudice the Federal Government because tradecraft used with earlier models does not become obsolete as systems are upgraded; the technical details about the equipment's core functions remains the same and/or can shed light on technical details about upgraded systems; and make/model information about earlier systems can shed light on the capabilities, limitations, and configurations of upgraded systems and their various components.

Category 1:

a. Disclosure of this category of information, on its own or in combination with other publicly available information, generally would provide adversaries with the information necessary to develop technologies to impede or negate the operation of particular cell site simulator systems. As basically the same equipment is used by Federal law enforcement agencies, including the FBI, such disclosure would have negative repercussions across the country and would put the public and the national security at risk as criminals and terrorists could actively work to thwart law enforcement efforts by developing defensive technologies to combat the effectiveness of this surveillance equipment or to render it non-functional altogether. Not only would this strip law enforcement of an effective tool for locating criminals and terrorists, it would endanger the lives of those victims (*e.g.*, kidnap victims) who otherwise could have been recovered if the gear was functional. Moreover, adversaries armed with this information, in combination with other publicly-available information, could construct and successfully operate their own cell site simulators against Federal, state, and local law enforcement, other Government entities, and the military, thus impeding effective functioning of the Government, law enforcement, and the military, all of which would endanger public safety and the national security.

Category 2:

a. Disclosure of this information, on its own, would reveal the relative capabilities – and correspondingly, limitations – of NYPD to electronically surveil and locate criminals and terrorists, and rescue/recover crime victims because it would reveal the specific resources available to the police department (as well as those not available to it). But disclosure of this information would not only implicate the equities and safety of the community in New York City. Combined with other information, disclosure of this information would permit the

development and honing of "heat maps" identifying the areas where particular technology and resources are utilized by law enforcement – *i.e.*, where criminals and terrorists can operate without fear of detection by cell site simulator technology – and those areas where they need to modify their behaviors (or that they need to avoid) because the likelihood that law enforcement will be able to locate them is greater. Thus, the information at issue in this category not only reflects on the resources that NYPD can bring to bear in its cases, but also adds critical information to the fund already available for criminals and terrorists to use in order to strategically navigate and thwart law enforcement on a broad scale.

b. Furthermore, disclosure of listings of particular components necessary to configure particular systems would also reveal tradecraft information about platforms and modes of operation of CSS equipment. Because this information would reveal not only the platforms and modes on which NYPD operates its gear specifically, but also the tradecraft capabilities of others using the gear including Federal law enforcement agencies, disclosure of this information would permit criminals and terrorists across the country to devise strategies to avoid the reach of the gear, develop technological countermeasures, and otherwise thwart the technology in order to circumvent local, state, and Federal law.

23. The FBI cannot publicly provide any greater specificity in the descriptions of the information protected, the reasons for protecting that information, or the risks of harm faced by its disclosure without disclosing the very information we have sought to protect, and thereby causing the harms we seek to prevent. However, the FBI is prepared to provide more detailed testimony on an *in camera, ex parte* basis to the Court should it determine that such a briefing would assist it in resolution of this matter.

CONCLUSION

24. As discussed above, the Federal Government has a significant interest in ensuring that cell site simulator technology remains a viable tool in enforcing criminal laws and protecting the security of the United States. Given the media attention to cell site simulators, the inability to control the unauthorized release of information in the internet age, and the ready access that criminals and terrorists have to any information published on the internet about this (and other) vital law enforcement techniques, disclosure of the information at issue in this case will jeopardize, if not vitiate, the FBI and larger law enforcement community's ability to successfully deploy this valuable technology to locate criminals and terrorists, and recover victims. Although some information about cell site simulators and their operation is publicly available, the specific capabilities, settings, limitations, tradecraft, and other types of information discussed herein and protected from disclosure in this case have not been authoritatively disclosed or confirmed by the FBI. Therefore, if such information is disclosed or endorsed here, criminal defendants and terrorists will gain valuable intelligence on the specific capabilities of the law enforcement community at large to effect surveillance of and locate individuals, which they can then use to effectively and successfully circumvent the law and/or disrupt or dismantle the equipment.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing it true and correct to the best of my knowledge.

Executed this 17th day of August, 2016 in Quantico, Virginia.

William Eric Chapman
Program Manager/
Information Technology Specialist
Tracking Technology Unit
Operational Technology Division
Federal Bureau of Investigation